Decision Support Systems 46 (2009) 815–825

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Studying users' computer security behavior: A health belief perspective

Boon-Yuen Ng [*], Atreyi Kankanhalli, Yunjie (Calvin) Xu

Department of Information Systems, National University of Singapore, Singapore

ARTICLE INFO

Available online 21 November 2008

Keywords:
Computer security
Security awareness
Health belief model
Email attachment
Virus

ABSTRACT

The damage due to computer security incidents is motivating organizations to adopt protective mechanisms. While technological controls are necessary, computer security also depends on individual's security behavior. It is thus important to investigate what influences a user to practice computer security. This study uses the Health Belief Model, adapted from the healthcare literature, to study users' computer security behavior. The model was validated using survey data from 134 employees. Results show that perceived susceptibility, perceived benefits, and self-efficacy are determinants of email related security behavior. Perceived severity moderates the effects of perceived benefits, general security orientation, cues to action, and self-efficacy on security behavior.

1. Introduction

Organizations increasingly rely on information systems for the transmission, processing, and storage of information. Hence, it is essential to protect the information within these systems and the availability of the computer systems. However, the increase in organizational dependence on information systems as well as the ease of mounting attacks has led to a corresponding increase in the number of security incidents and damage caused [26]. A computer security incident is defined as a security-related adverse event in which there is a loss of information confidentiality, disruption of information or system integrity, disruption or denial of system availability, or violation of any computer security policies [19]. According to the 2007 annual survey conducted by the Computer Security Institute [36], 46% of respondents indicated that their organization experienced a security incident within the last 12 months. Of these, a significant number (52%) of the attacks are virus-related. It is therefore important for organizations and employees to be aware of and protect themselves against security threats and cybercrime.

Chung et al. [8] described three approaches at a national level to fight against cybercrime, i.e., legal, organizational, and technological. Countries around the world have created laws (e.g., Computer Misuse Act in Britain and Singapore) and set up national agencies (e.g., the Computer Analysis Response Team in the US) to combat computer security threats. Various technologies are applied at the national level for this purpose, such as a computer surveillance system developed by the FBI. Further, organizational measures are important in this fight. Organizations need to develop and implement a multi-dimensional approach to safeguard their information assets [52].

Among the approaches, technological measures such as firewalls for perimeter defense are common in organizations. Such solutions are necessary but not sufficient for protection [35]. This is because success of computer security depends on the effective behavior of users [43]. Employees in an organization play an essential role in the prevention and detection of security incidents. While system administrators are responsible for configuring firewalls and servers in a secure manner, users are responsible for practicing security countermeasures such as choosing and protecting appropriate passwords.

Thus, for effective security, users have to make a conscious decision to comply with the organization's security policies and adopt computer security behavior. To this end, organizations have been implementing security training and awareness programs to educate users [35]. While many practitioner guidelines are available, there is a lack of empirical studies concerning the design and effectiveness of security awareness programs. An effective awareness program should influence a user's attitude and behavior to be more security-conscious [47]. Thus, it is critical to understand what will influence a user's security behavior so that appropriate awareness programs can be designed. However, there is little theoretically grounded empirical information systems research on the behavior of individuals in practicing secure computing.

Motivated by such theoretical and practical concerns, our research question is, “What are the salient influences for a user to practice computer security in an organization?” Through this study, we aim to contribute to the better understanding of security behavior of computer users in organizations, so that the security climate of an organization can be improved. By identifying and understanding the determinants of computer security behaviour, interventions can be designed to change behaviour by directing at one or more of the determinants.

[*] Corresponding author.
E-mail addresses: ngby@comp.nus.edu.sg (B.-Y. Ng), atreyi@comp.nus.edu.sg (A. Kankanhalli), xuyj@comp.nus.edu.sg (Y.(C.) Xu).

0167-9236/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2008.11.010

With the paucity of theoretical perspectives in this area, this study draws upon relevant literature from other fields. Specifically, it makes use of the well-known health belief model [40] traditionally employed to explain preventive healthcare behavior. This perspective is applicable because security practices can be seen as preventive behavior to avert security incidents. The model suggests that an individual's behavior is determined by the threat perception and evaluation of the behaviour to resolve the threat. This model offers a new perspective to better understand the phenomenon using constructs that have not been previously explored in IS research, such as cues to action and general security orientation. Our research model is tested by surveying 134 employees from multiple organizations. The findings are expected to inform theory and practice in this area.

2. Conceptual background

2.1. Computer security behavior

There are relatively few research studies of security behavior of computer users and how behavior can be modified to practice security countermeasures. Previous studies in this area can be categorized according to their context, i.e., organizational or non-work use of computers. An example of a study in the organizational context is the investigation of end-user security behaviors and their antecedents by Stanton et al. [43]. It reveals relationships between end-user security behavior (such as password management, non-work-related computing behavior, and obtaining security training) and a combination of situational factors (such as organizational type) and personal factors (such as income level and job role). The study provides empirical insights but without theoretical bases. Yet another study in the organizational context by Aytes and Connolly [4] proposes a conceptual model of user security behavior based on risk perception. Of the rare theoretically-grounded empirical studies in this context is the study by Chan et al. [7], which explores the influence of security climate and self-efficacy on user compliance to security policies. Thus there is a lack of studies that comprehensively model and test the individual beliefs that influence computer security behavior in organizations, which is broader than compliance to organizational security policies.

Other related studies pertain to computer users in a non-work environment, which differ from organizational settings by the absence of managerial interventions and controls. For example, the factors that influence a home user's intention to practice computer security have been investigated by applying the decomposed theory of planned behavior [33]. Findings indicate that family, peer, and mass media influence, perceived usefulness, and self-efficacy are important factors that influence a home user's intention to practice computer security. Another empirical study in the non-work context surveyed students to investigate determinants of safe online behavior [29]. It finds significant influences from online safety involvement, self-efficacy, and personal responsibility but without a theoretical explanation. In another study of college students, application of protection motivation theory borrowed from healthcare showed that self-efficacy predicts online consumers' intention to practice safe online behavior, such as updating virus protection [28]. With the lack of theoretically-grounded empirical studies of determinants of computer security behavior in organizations, we now review theories that may be applicable for our study.

2.2. Applicability of IS adoption theories

Information systems (IS) research is rich in theories pertaining to technology adoption. Computer security behavior includes the adoption and use of security technologies such as anti-virus software and firewalls. Theories such as Technology Acceptance Model [14] and Theory of Planned Behavior [3] can be applied to study users' intention to use security technologies (e.g., [33]). However, recent research in security behavior has revealed that there are significant differences between positive technologies (used for designed utilities) and protective technologies (used to prevent negative consequences) [15]. Security technologies generally belong to the category of protective technologies as they are used to avert undesirable incidents, such as virus attacks. This recent discussion gives the impetus to look for theories that are more suitable to study the use of such protective technologies.

In addition, computer security behavior involves more than just the adoption of technology. While the use of protective technologies is critical, computer security behavior also includes other behaviors such as the choice of strong passwords, regular backing up of data, and exercising caution with suspicious email attachments. Such behaviors do not involve the adoption of any specific technology but require the computer user to consciously decide to perform additional steps for the sake of preventing unwanted situations such as loss of data. For

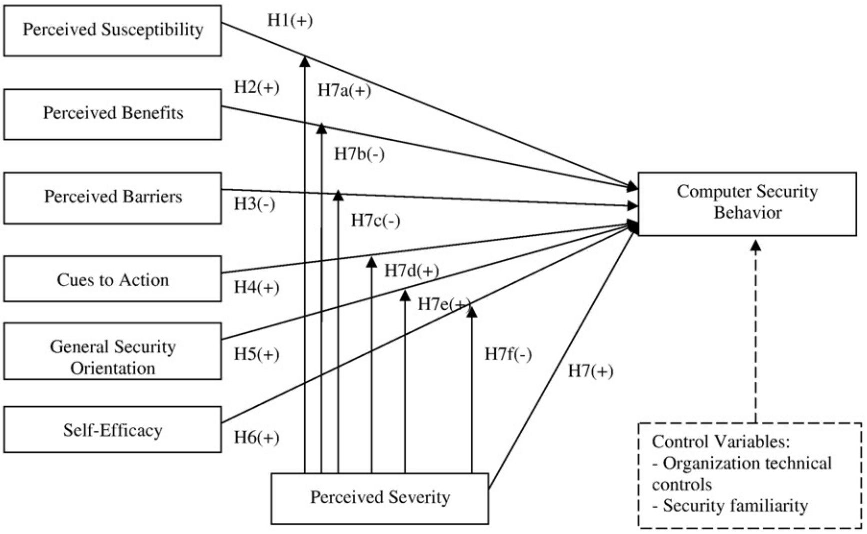

Fig. 1. Research model.

such behaviors, IS theories such as Technology Acceptance Model may be less suitable. Behavioral theories such as Theory of Planned Behavior provide a general framework to study user intentions, but more could be done to explore determinants that are more specific to security behavior.

With the paucity of theoretical perspectives in information systems on practicing computer security, most research studies have turned to theories in other domains. A domain that has been borrowed from is healthcare. In the non-work context, security behavior of home wireless network users has been investigated using the protection motivation theory [51]. This theory has previously been used in healthcare to explain a person's coping behavior when he/she is informed of a threatening event. This and other studies (e.g., [27,28]) suggest the applicability of healthcare theories to study computer security behavior. The similarities between preventive healthcare and protective security behavior are described below.

2.3. Relevance of healthcare behavioral theories

Parallels can be drawn between protective security behavior (such as using a strong password to prevent unauthorized use of one's account) and preventive healthcare behavior (such as observing a healthy diet to avoid heart diseases). Preventive healthcare refers to behaviors that will prolong an individual's healthy life or practices that otherwise lessen the effects of diseases [25]. Protective security behavior refers to behaviors that will reduce the risk and/or impact of security incidents. There are a number of characteristics of preventive healthcare common to practicing security countermeasures. Both involve practicing preventive and protective behavior to avert an unwanted situation. The success of preventive healthcare and security practices is seen in the non-occurrence of diseases (for preventive healthcare) and security incidents (for security practices) respectively. The occurrence of diseases disrupts the normal functioning of one's body whereas the occurrence of security incidents disrupts the functioning of one's computer system and possibly affects the organization. Practicing preventive healthcare and security countermeasures both create inconveniences for the individuals in terms of extra effort.

Most of the theories on preventive healthcare behavior use an expectancy-value approach. Expectancy refers to beliefs about how well a person can perform a task or activity, and value refers to the incentives or reasons for performing that task or activity [16]. According to the basic expectancy-value theory, a person's attitude towards a behavior is a function of the perceived likelihood of outcomes associated with the behavior and the expected value or

Table 1
Constructs and items

Construct	Item	Source
Behavior (BEH)	BEH1: Before reading an email, I will first check if the subject and the sender make sense. (agree/disagree)	[38]
	BEH2: Before opening an email attachment, I will first check if the filename of the attachment makes sense. (agree/disagree)	[38]
	BEH3: I exercise caution when I receive an email attachment as it may contain a virus. (agree/disagree)	Self-developed
	BEH4: I do not open email attachments if the content of the email looks suspicious. (agree/disagree)	Self-developed
Perceived susceptibility (SUS)	SUS1: The chances of receiving an email attachment with virus are high. (agree/disagree)	[6]
	SUS2: There is a good possibility that I will receive an email attachment with virus. (agree/disagree)	[6]
	SUS3: I am likely to receive an email attachment with virus. (agree/disagree)	[6]
Perceived severity (SEV)	SEV1: Having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me. (agree/disagree)	[51]
	SEV2: Losing organizational data as a result of opening a suspicious email attachment is a serious problem for me. (agree/disagree)	[51]
	SEV3: If my computer is infected by a virus as a result of opening a suspicious email attachment, my daily work could be negatively affected. (agree/disagree)	Self-developed
Perceived benefits (BEN)	BEN1: Checking if the sender and subject make sense is (definitely/not) effective in preventing viruses from infecting my computer.	Self-developed
	BEN2: Checking if the filename of the email attachment makes sense is (definitely/not) effective in preventing viruses from infecting my computer.	Self-developed
	BEN3: Exercising care before opening email attachments is (definitely/not) effective in preventing viruses from infecting my computer.	Self-developed
Perceived barriers (BAR)	BAR1: Exercising care when reading emails with attachments is inconvenient. (agree/disagree)	Self-developed
	BAR2: Exercising care when reading emails with attachments is time-consuming. (agree/disagree)	[6,51]
	BAR3: Exercising care when reading emails with attachments would require considerable investment of effort other than time. (agree/disagree)	[51]
	BAR4: Exercising care when reading emails with attachments would require starting a new habit, which is difficult. (agree/disagree)	[6]
Cues to action (CUE)	CUE1: My organization distributes security newsletters or articles. (never/always)	Self-developed
	CUE2: My organization organizes security talks. (never/always)	Self-developed
	CUE3: My organization's IT helpdesk sends out alert messages/emails concerning security. (never/always)	Self-developed
	CUE4: My organization constantly reminds me to practice computer security. (agree/disagree)	Self-developed
General security orientation (GEN)	GEN1: I read information security bulletins or newsletters. (agree/disagree)	Self-developed
	GEN2: I am concerned about security incidents and try to take action to prevent them. (agree/disagree)	[25]
	GEN3: I am interested in information about computer security. (agree/disagree)	[25]
	GEN4: I am constantly mindful about computer security. (agree/disagree)	Self-developed
Self-efficacy (SEF)	SEF1: I am confident of recognizing a suspicious email. (agree/disagree)	Self-developed
	SEF2: I am confident of recognizing suspicious email headers. (agree/disagree)	Self-developed
	SEF3: I am confident of recognizing suspicious email attachment filename. (agree/disagree)	Self-developed
	SEF4: I can recognize a suspicious email attachment even if there was no one around to help me. (agree/disagree)	[7,12]
Technical controls (CON1)	My organization ensures that my computer is protected from viruses by installing anti-virus software on my computer and/or the email server. (agree/disagree)	Self-developed
Security familiarity (CON2)	How would you rate yourself in terms of familiarity with computer security practices? (very familiar/not at all familiar)	Self-developed

evaluation of those outcomes. The overall desirability of behavior is based on the summed products of the expectancy and value of outcomes. Several well-known behavioral models have their roots in expectancy-value theories, such as social cognitive theory, protection motivation theory, and the health belief model. The next section describes why we chose the health belief model as the lens for our study.

2.4. Health belief model

A popular expectancy-value model used in healthcare is the health belief model. It is one of the earliest comprehensive attempts to explain healthcare behavior based on expectancy value principles [40]. It has been widely applied to all types of healthcare behavior, such as contraceptive use, diet, and exercise. It has also been applied in other diverse areas, such as preventive behavior against piracy threat facing US firms [22] and emigration intention [20]. The model appears to have implications for work motivations as well as a broad range of human behaviors [49].

The health belief model identifies two considerations in an individual's decision to adopt healthcare behavior in response to the threat of illness, i.e., perceptions of illness threat and evaluation of behavior to resolve this threat. Perception of illness threat depends on two beliefs, i.e., the *perceived susceptibility* to the illness and *perceived severity* of the illness. Evaluation of behavior depends on assessing the *perceived benefits* of the healthcare behavior to prevent the illness and the *perceived barriers* to performing the preventive healthcare behavior in order to compute the perceived net benefit [13]. Apart from perceived susceptibility, perceived severity, perceived benefits and perceived barriers, three other variables included in the health belief model are self-efficacy, cues to action, and general health orientation. *Self-efficacy* is a person's self-confidence in his ability to perform a behavior. This concept originates from the social cognitive theory [5] and describes individuals' responses to the challenges of changing habitual unhealthy behaviors. *Cues to action* are triggers that make the individual take action, such as health education and advice from others [24]. *General health orientation* refers to the individual's predisposition to healthcare behavior [49]. This construct captures the individual's tendency towards performing healthy behaviors.

Table 3
Descriptive statistics of constructs and inter-construct correlations[a]

Construct	Mean	SD	BEH	SUS	SEV	BEN	BAR	GEN	CUE	SEF
BEH	6.03	0.82	0.56							
SUS	4.86	1.28	0.41	0.76						
SEV	5.42	1.05	0.33	0.36	0.64					
BEN	5.56	0.98	0.53	0.31	0.39	0.63				
BAR	3.64	1.38	−0.07	0.14	0.16	0.04	0.72			
GEN	5.22	1.16	0.17	0.10	0.22	0.09	−0.05	0.78		
CUE	4.96	1.44	−0.04	−0.11	0.23	0.05	0.05	0.36	0.80	
SEF	5.22	1.14	0.40	0.08	0.05	0.11	−0.15	0.16	−0.01	0.78

[a] Square root values of average variance extracted are indicated on the diagonal cells.

Table 2
Demographics of respondents

Demographic	Category	Percentage
Age	20–29	54.6%
	30–39	33.1%
	40–49	10%
	>=50	2.3%
Gender	Male	50.7%
	Female	49.3%
Job title	Senior management	2.2%
	Middle management	15.7%
	First-level supervisor	20.9%
	Technician	6.7%
	Analyst	16.4%
	Administrative support	17.2%
	Others	20.8%
Functional area of job	Accounting	2.2%
	Administration	9.7%
	Information Technology	47.8%
	R&D	9.7%
	Operations	9.7%
	Marketing and Sales	8.2%
	Others	12.6%
Job tenure at current organization	<1 year	3.1%
	1–2 years	45%
	3–5 years	25.2%
	6–10 years	19.8%
	11–20 years	3.8%
	>20 years	2.3%
Industry type of organization	Government	19.4%
	Education	18.7%
	Finance/Banking	3.0%
	Information Technology	34.3%
	Telecommunications	6.0%
	Health/Medical	2.2%
	Military	1.5%
	Others	14.9%
Organization size	1–20	6.0%
	21–50	13.4%
	51–100	7.5%
	101–500	9.7%
	501–1000	11.2%
	>1000	52.2%

The health belief model is comprehensive in including a number of explanatory constructs that are not represented in IS adoption or other healthcare theories, but important in computer security practice. The constructs perceived susceptibility, perceived severity, cues to action and general health orientation are not present in prior IS adoption theories, while cues to action and general health orientation are not present in other healthcare theories. One of the most important components of individual security behavior is the effective management of risk. Risk management requires the identification of threats and determination of the likelihood and impact of threats [44]. This is similar to the concepts of perceived susceptibility and perceived severity in the health belief model.

Further, the constructs of general health orientation and cues to action are likely to be relevant to computer security behavior. Cues to action could include the organization's security awareness efforts. General health orientation is analogous to an individual's general orientation or predisposition to security. Applying this idea to the security domain, this construct is mapped to an individual's "security-consciousness" or *general security orientation*. To the best of our knowledge, these two constructs have not been explored in past security behavior studies. Hence, we apply the health belief model as an overarching theory to explain a user's computer security behavior in an organization. In the next section, we elaborate on our research model.

3. Research model

Fig. 1 presents our research model. While most studies based on the health belief model consider behavioral intention or likelihood of behavior as the dependent variable, we use self-reported actual behavior instead. Although this variable is subject to self-report bias, it is often easier to self-assess than intention and more objective. This approach has been taken in a few previous empirical preventive healthcare studies (e.g., [25]) by asking respondents what behaviors they engage in. Hence, self-reported computer security behavior constitutes our dependent variable. We define each construct and present the related hypotheses below.

3.1. Perceived susceptibility

In the health belief model, this construct refers to the "subjective risks of contracting a condition" [39, p. 99]. Individuals vary widely in their perceived susceptibility. For example, an individual may deny any possibility of contracting the condition, another may recognize the statistical probability, and yet another may feel that he is in real danger of contracting the condition. Similarly, in the security domain, individuals may respond very differently even if they are presented the same facts or statistics, and this may influence their security behaviour. Given the same information about the probability of a security incident, one may feel that the likelihood is high while another may feel that it will never happen. In this context, perceived susceptibility refers to a user's perceived likelihood of a security incident taking place. When an individual perceives greater susceptibility to security incidents, he will be likely to exhibit a greater level of computer security behavior. Hence, we hypothesize:

H1. Perceived susceptibility to security incidents is positively related to computer security behavior.

3.2. Perceived benefits

In the health belief model, perceived benefits refer to an individual's beliefs regarding the relative effectiveness of an action to reduce the disease threat. It is the individual's beliefs about availability and effectiveness of various courses of action, not the objective facts about the benefits, that determine a person's health behaviour [39]. Here, perceived benefits refer to a user's belief in the perceived effectiveness of practicing computer security. Thus, higher perceived benefits are likely to lead to greater computer security behavior. We hypothesize:

H2. Perceived benefits of practicing computer security are positively related to computer security behavior.

Table 4
Reliability and validity tests

Construct and items	Loading	*t*-value	Cronbach alpha
BEH			0.65
BEH1	0.49***	5.31	
BEH2	0.53***	5.77	
BEH3	0.53***	5.79	
BEH4	0.67***	7.49	
SUS			0.78
SUS1	0.60***	6.96	
SUS2	0.89***	11.05	
SUS3	0.75***	9.07	
SEV			0.67
SEV1	0.72***	7.76	
SEV2	0.58***	6.16	
SEV3	0.61***	6.48	
BEN			0.65
BEN1	0.56***	6.09	
BEN2	0.68***	7.62	
BEN3	0.62***	6.81	
BAR			0.80
BAR1	0.60***	7.13	
BAR2	0.90***	11.59	
BAR3	0.66***	7.89	
BAR4	0.68***	8.29	
GEN			0.85
GEN1	0.71***	9.07	
GEN2	0.85***	11.60	
GEN3	0.65***	8.04	
GEN4	0.87***	11.94	
CUE			0.87
CUE1	0.87***	12.18	
CUE2	0.70***	8.92	
CUE3	0.79***	10.45	
CUE4	0.83***	11.34	
SEF			0.86
SEF1	0.61***	7.35	
SEF2	0.82***	11.06	
SEF3	0.86***	11.76	
SEF4	0.83***	11.12	

*** $p<0.001$.

3.3. Perceived barriers

Although a person may believe that a given action is effective in reducing threat, he may find that action to be inconvenient or unpleasant to him. These negative aspects are the perceived barriers to action [39]. In a meta-analysis of the applications of health belief model to preventive healthcare behaviors, perceived barriers was a significant predictor compared to the other determinants [24]. Similar to preventive healthcare behaviour, computer security behaviour often causes inconvenience because of additional controls or measures required, such as two-factor authentication instead of a simple password authentication. Here, we define perceived barriers as a user's perceived cost and inconvenience of practicing computer security, which is likely to reduce the performance of computer security behavior. Hence, we hypothesize:

H3. Perceived barriers of practicing computer security are negatively related to computer security behavior.

3.4. Cues to action

Rosenstock [39] argues that healthcare action may not take place unless "some instigating event occurred to set the process in motion" [39, p. 101]. These events are the cues to actions. Examples of cues to action include internal perceptions of symptoms, impact of communications media, knowledge of someone suffering from a similar disease, or reminders from doctors. In our context, cues to action refer to experiences or triggers that would motivate and activate a user to practice computer security. Examples include exposure to security awareness programs, media cues, social influences and recommendations from experts. In this study, we focus on organizational efforts such as security awareness programs as we are interested to study how employee's security behavior can be encouraged in an organizational context. An organization's efforts in security awareness reflect its management's commitment towards security and the expectations it has from employees. Greater cues to action are likely to lead to increased computer security behavior. Hence, we hypothesize:

H4. Cues to action are positively related to computer security behavior.

3.5. General security orientation

In the health belief model, general health orientation refers to "the individual's predisposition or habit concerning health seeking behaviour in general" [49, p. 188]. It is not related to the anticipated consequences of healthcare behavior but is an individual's generalized response tendency. Another study proposed a similar construct named *health consciousness*, defined as "the degree to which health concerns are integrated into a person's daily activities" [25, p.10]. In the context of computer security, we label the construct as general security orientation. This refers to a user's predisposition and interest concerning practicing computer security. Individuals with higher levels of health consciousness have been observed to exhibit greater levels of preventive healthcare behaviors [25] and a similar relationship is expected between general security orientation and computer security behavior. Hence, we hypothesize:

H5. General security orientation is positively related to computer security behavior.

Table 5
Regression models

Model	Model 1	Model 2	Model 3		
	Main effects	Interaction effects	Full		
Variables	Coefficient	Coefficient	Coefficient	*t*-value	Results
Perceived susceptibility	0.22**	0.21**	0.23**	3.48	H1 supported
Perceived Benefits	0.39***	0.39***	0.39***	5.58	H2 supported
Perceived Barriers	−0.08	−0.09	−0.08	−1.24	H3 not supported
Cues to Action	−0.08	−0.06	−0.10	−1.49	H4 not supported
General Security Orientation	0.07	0.12	0.11	1.46	H5 not supported
Self-efficacy	0.31***	0.35***	0.33***	5.02	H6 supported
Perceived Severity	0.10	0.11	0.09	1.10	H7 not supported
Perceived Severity × perceived susceptibility		0.06	0.06	0.88	H7a not supported
Perceived Severity × Perceived Benefits		−0.17*	−0.16*	−2.16	H7b supported
Perceived Severity × Perceived Barriers		0.11	0.10	1.58	H7c not supported
Perceived Severity × Cues to Action		0.17**	0.18**	2.86	H7d supported
Perceived Severity × General Security Orientation		0.17**	0.19**	2.78	H7e supported
Perceived Severity × self-efficacy		−0.19**	−0.18**	−2.88	H7f supported
Technical controls (control variable)			0.13	1.77	
Security familiarity (control variable)			0.00	0.06	
Dummy variable for student			0.02	0.26	
R^2	0.479	0.593	0.605		
Change in R^2		0.114	0.012		
Adjusted R^2	0.450	0.549	0.551		

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$.

3.6. Self-efficacy

Self-efficacy is another antecedent in the health belief model [41] and a useful predictor of healthcare behavior [1]. The roots of self-efficacy come from social cognitive theory and it refers to an individual's self-confidence in his ability to perform a behavior [5]. According to social cognitive theory, individuals with greater confidence in their abilities are more likely to initiate challenging behaviors such as smoking cessation [37]. Self-efficacy, when applied in the area of computer training, was found to exert a strong influence on individuals' performance in a computer training course [11]. In this study, self-efficacy refers to a user's self-confidence in his/her skills or ability in practicing computer security, which is likely to increase computer security behavior. This leads us to our next hypothesis:

H6. Self-efficacy is positively related to computer security behavior.

3.7. Perceived severity

In the health belief model, this construct refers to a person's conviction concerning the seriousness of a given health problem. Perceived seriousness is not limited to the clinical consequence of a health problem, but may extend to the implications on the individual's job or family [39]. Similarly, in computer security, a person's perceived seriousness of a security incident is not limited to the damage to systems and data, but also the implications on the person's job or organization. This is particularly so in the organizational context as the data that is affected by a security incident is likely to be owned by the organization. Loss of confidentiality, integrity, or availability of organizational data may affect the organization negatively and disrupt employees' work. An employee who did not practice computer security, thus resulting in security incidents, may also be held responsible by the organization. Though the consequences of a security incident may be severe, individual employees may have a different perception of the severity or extent of the damage. We define perceived severity to be a user's perceived seriousness of a security incident, which should lead to greater computer security behavior. We hypothesize:

H7. Perceived severity of security incidents is positively related to computer security behavior.

Of all the above determinants, we believe perceived severity moderates the effects of the other determinants. This is based on the roots of the Health Belief Model, i.e., the basic expectancy-value theory that the desirability of behavior is based on the summed products of the expectancy and value of outcomes. Perceived severity can be regarded as valence or value in Vroom's [48] expectancy theory for motivation. Vroom defines motivation as an interaction between expectancy and value, which refers to the valence to the individual of the outcomes. The main objective of practicing computer security is to avert negative consequences, and hence the valence of the behavior is the perceived severity or consequences of negative outcomes. Perceived severity is a weighting factor in influencing other variables' effects on computer security behavior.

A study using Health Belief Model to predict health behaviors in college students hypothesized that perceived threat (the combination of perceived severity and perceived susceptibility) affects health behavior [2]. A meta-analytic review of the protection motivation theory suggests that perceived severity of the disease may influence the role of perceived vulnerability, which is the same as perceived susceptibility in the Health Belief Model [30]. As risk is based on the likelihood of threat (similar to susceptibility) multiplied by the impact of threat (similar to severity) [44], we hypothesize that perceived severity magnifies the effect of perceived susceptibility:

H7a. Perceived severity increases the positive effect of perceived susceptibility on computer security behavior.

Additionally, we hypothesize that perceived severity reduces the effects of perceived benefits and perceived barriers. In the face of a severe threat, the effects of perceived benefits and perceived barriers become less important. If a person believes that the negative consequences are significantly severe, he is likely to practice the countermeasures even if he thinks that the countermeasures may not be fully effective because some protection is better than no protection. Similarly, when consequences are severe, it will outweigh the cost of any inconvenience in practicing the countermeasures. This leads us to the next two hypotheses:

H7b. Perceived severity reduces the positive effect of perceived benefits on computer security behavior.

H7c. Perceived severity reduces the negative effect of perceived barriers on computer security behavior.

When a person perceives a threat to be severe, cues to action are even more likely to trigger him into action. In other words, perceived severity and cues to action are likely to have a synergistic effect on computer security behavior. Similarly, a person who is highly conscious of security is even more likely to act if he perceives the threat to be severe. The higher consciousness may make the individual more proactive in computer security behavior when the perceived severity of threat is higher. Hence, we hypothesize:

H7d. Perceived severity increases the positive effect of cues to action on computer security behavior.

H7e. Perceived severity increases the positive effect of general security orientation on computer security behavior.

Finally, we hypothesize that perceived severity reduces the effect of self-efficacy. If a person perceives the threat to be severe, he is more likely to attempt practicing the countermeasure even if he is not fully confident of his ability to do so, as the negative consequences of the threat drives him into action. This leads us to our last hypothesis:

H7f. Perceived severity reduces the positive effect of self-efficacy on computer security behavior.

In addition to the above constructs, we measure the organization's technical controls as a control variable. Past literature has suggested that the presence of technical controls may lead to users having less concern for security as they may perceive that adequate security controls are in place [46]. Another control variable is the familiarity with computer security practices. This acts as a control for the individual's prior knowledge and skills in computer security. Hence, these two variables are added as control variables to rule out possible rival explanations and improve the internal validity of this study [45].

4. Research methodology

The model was quantitatively tested using the survey methodology [32]. The survey instrument was developed following procedures recommended by Churchill [9]. The first step was to specify the domain of the construct. The second step was to generate items that capture the domain as specified. The constructs were operationalized by adapting items from past literature whenever possible. After considering the original definitions of the constructs in the health belief model, we referred to academic and industry security literature and adapted the constructs for the security behavior domain. Pre-tests of the items were conducted with experts in the field. Finally, sorting procedures for the conceptual validation of the instrument [31] were conducted.

4.1. Operationalization

Many of the studies applying the health belief model till now have been characterized by poor operationalization of constructs and failure to assess construct validity and reliability. In particular, some studies suffered from problems of multi-dimensionality in operationalizing the model (e.g., [1]). Hence, care was exercised when borrowing items from past studies to ensure rigor in our methodology.

Challenges were also faced in adapting these constructs to the context of computer security. One of these challenges was in measuring computer security behavior. Safe computing behavior involves a wide range of specific behaviors, which if combined in one variable will pose multidimensionality problems. Hence, we measure one common practice as a representation of security behavior, i.e., *exercising care when reading emails with attachments*. Organizations generally permit members to have email access. It is thus important to be careful when reading emails, as virus attacks are one of the most reported causes of financial loss [18] and typically spread through email. Even though computers may be running anti-virus software, new viruses may not be detected by the software. Suspicious emails, such as those from unknown sources or with unsolicited attachments, should not be read [38]. Thus, items for this construct measure if users check for suspicious email headers, attachment filenames, or email content before opening an attachment. We also added an overall item that measures whether a user exercises caution when he/she receives an email attachment.

4.2. Conceptual validation of instrument

Instrument validation consists of assessing content, conceptual, and construct validity, and reliability [45]. Content validity is ensured

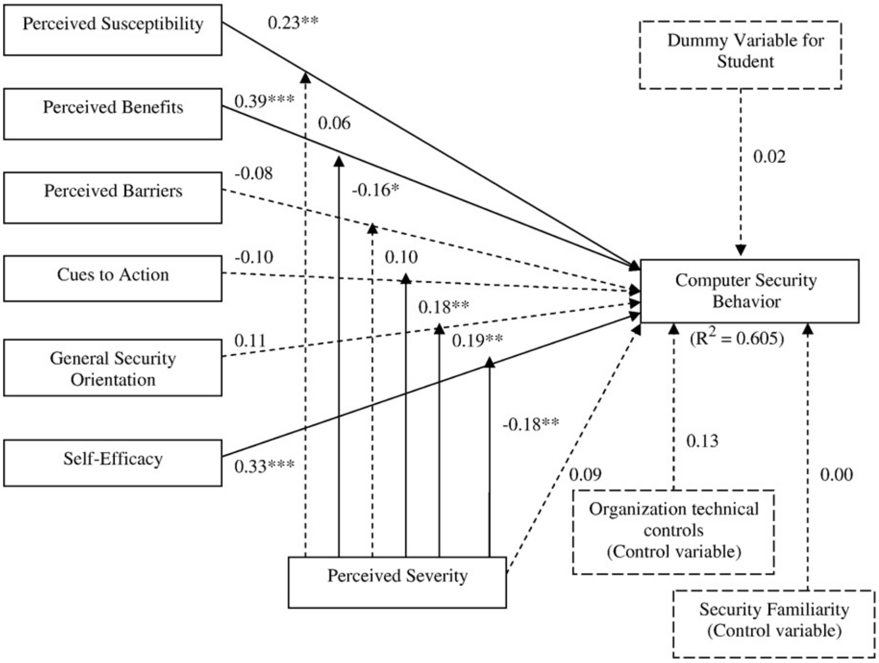

Fig. 2. Graphical display of results. (* $p<0.05$, **$p<0.01$, ***$p<0.001$).

by drawing representative questions from a universal pool. Hence, items were generated by drawing from past literature in security behavior and adapting items from literature in healthcare behavior. In addition, pre-tests of the items were conducted by interviewing academic as well as industry experts in this field. Items were developed and refined based on the comments gathered from the pre-tests.

Conceptual validity can be assessed by using the sorting procedures proposed by Moore and Benbasat [31]. Here, we describe the process and results of the sorting procedures. In the first round of sorting (unlabelled), four judges sorted items into self-created categories as they were not told what the underlying constructs were. The level of agreement between judges was measured using Cohen's Kappa. A second measure of validity is the overall placement ratio of items placed within the target construct [31]. This round was repeated with a different set of judges after some items were refined to improve the clarity. For the third round (labeled), another four judges were recruited and given the labels and definitions of the constructs before the sort. Kappa scores averaged 0.83 while the overall placement ratio of items within target constructs was 93%. Thus, we conclude that the instrument development process resulted in scales that demonstrated high conceptual validity. Table 1 shows the final list of items. All items are anchored on 7-point Likert scales.

4.3. Survey administration

Following the development of the instrument, the survey questionnaire was prepared. To reduce measurement error, care was taken in preparing the questionnaire layout, the question format, and the question order [32]. The questionnaire was designed to be clear and neat. Color paper was used to give a professional appearance. Detailed instructions with examples were provided. Identifying information (the name of the university conducting the research) was prominently displayed on the questionnaire for credibility enhancement.

Numeric labels were used for each item, but verbal labels were provided in the examples found in the instructions to help all respondents interpret the scales consistently and to produce more reliable measurement [42]. Questions were organized into sections to minimize confusion of respondents and an introductory statement about the section was provided to orient the respondents [32]. Respondents were also informed that this survey pertains to their use of email in their respective organizations; this helped the respondents to interpret the questions in the intended organizational context. To reduce errors arising from common method bias, the presentation order of items was shuffled within the section.

The survey was administered to part-time (working) students in two computing classes at a large public university and individuals employed in three IT-related organizations to which we had access, providing a sample of 134 employees. The response rate approximated 31%. The questions were administered in paper form at the end of class or at the office location where the respondents worked. The responses were returned back to the researchers directly after completion without any intermediaries. A small token incentive was given to respondents who completed the survey to encourage response. All questionnaires were checked to make sure responses were complete. Table 2 summarizes the demographics of the sample and the characteristics of the organizations represented by the survey respondents. Table 3 shows the descriptive statistics for all constructs and the inter-construct correlations.

5. Data analysis

Multiple regression analysis is a flexible and adaptable multivariate technique that can be used to examine the relationship between a single dependent variable and a set of independent variables [21]. It is also the recommended approach for testing interactions with continuous variables [10]. Hence, we used moderated multiple regression to test our model with interaction hypotheses [23]. We first established the reliability and construct validity of our instrument before we proceeded to test the hypotheses using regression. The assumptions of regression were also tested.

5.1. Construct validity and reliability

With multiple indicators measuring each construct, construct validity is important to ensure that the various indicators operate in the intended manner. Reliability refers to dependability, which means that the results produced by indicators are consistent and do not vary because of the measurement process [32]. Cronbach Alpha reliability coefficient was used to test the reliability of the items. For internal consistency, Cronbach Alpha should have a value of at least 0.707 [34]. However, for exploratory studies, such as ours, a minimum alpha value of 0.6 is allowable [34]. Table 4 summarizes the factor loadings (for construct validity) and reliability test results. Although one item (BEH1) demonstrates factor loadings less than 0.5 which is the recommended threshold [21], dropping this item decreases the Cronbach Alpha. Since its loading is significant at 0.001 level, this item is retained. Since all constructs exhibited acceptable construct validity and reliability, we proceeded to test the hypotheses.

5.2. Hypotheses testing

Table 5 shows the regression models that we ran. As per moderated multiple regression procedures, the first model tested the main effects, the second model included the interaction terms, and the third (full) model included the control variables as well. Table 5 and Fig. 2 show the results of hypotheses testing using moderated multiple regression techniques. Examination of the tolerance values and the variance inflation factors indicated that multicollinearity was not a problem [21]. When adding the control variables (technical controls of the organization and the individual's familiarity with computer security practices), no significant change was observed in the model. We also added a dummy variable to indicate whether the respondents were part-time (working) students or non-student employees. The control variables and the dummy variable were not significant. The explanatory power (R^2) for the model with main and moderating effects was 0.59, which is well above the acceptable threshold of 10% [17]. The two control variables and the dummy variable explained an additional variance of 1% in the dependent variable. The results indicated that perceived susceptibility, perceived benefits, and self-efficacy were significant in determining individuals' computer security behavior, i.e., H1, H2, and H6 were supported. However, perceived barriers, cues to action, general security orientation, and perceived severity were not significant determinants of individuals' computer security behavior, i.e., H3, H4, H5, and H7 were not supported. Furthermore, perceived severity moderated the effects of perceived benefits, cues to action, general security orientation, and self-efficacy, i.e., H7b, H7d, H7e and H7f were supported. The moderating effects of perceived severity on perceived susceptibility and perceived barriers were not significant, i.e., H7a and H7c were not supported. In total, 7 out of 13 hypotheses were supported.

6. Discussion

6.1. Discussion of results

The results of the study show that perceived susceptibility, perceived benefits, and self-efficacy are determinants of a user's computer security behavior, when applied to exercising care with email attachments. The first two results are consistent with the nature of security as the motivation for security is to mitigate risks and reduce threat likelihood [44]. Self-efficacy is also important, as a computer user must be confident and able to perform the necessary mitigation measures. In fact, a meta-analysis of the prediction of health behavior shows that self-efficacy, of all variables, was most strongly related to intention and behavior [30]. This study highlights the importance of self-efficacy as well.

Our findings show that the main effects of perceived barriers, cues to action, general security orientation, and perceived severity are not significant. Security is usually viewed as an inconvenience, which may deter users from practicing safe behavior. However, for this particular study, the mean of the perceived barriers construct is lower than the other constructs (refer to Table 3), indicating that users did not find much barriers or inconvenience in practicing safe email behavior. Since the survey respondents were quite IT-savvy, as they were part-time (working) computing students and/or work in IT-related organizations, they might not find it difficult to practice secure email behavior.

Our findings indicate that cues to action, in particular organizational efforts such as awareness programs, are not significant in triggering a person to behave in a secure manner. This does not rule out other forms of cues to action, such as individual experience or other forms of communications external to the organization, which are not measured in this study. The results also indicate that a person's general security orientation is not significant in determining security behavior. However, these effects are significant when moderated by perceived severity.

Our findings indicate that perceived severity is not a significant determinant of security behavior. This is not a surprising finding as some of the past studies in health behavior have shown perceived severity to be a weak direct predictor of health behavior [30]. Although the main effect of perceived severity is not significant, it magnifies the effects of cues to action and general security orientation. This indicates contingency effects, that is, the effects of these factors alone may not be effective in pushing one to practice security, but the combination of these factors may lead to computer security behavior. Perceived severity is not significant on its own, but operates with multiple other factors to influence computer security behavior.

As hypothesized, perceived severity reduces the effect of perceived benefits and self-efficacy. This implies that when perceived severity is high, perceived benefits and self-efficacy are not as important in determining one's decision to practice security. Although perceived severity does not have a significant main effect, the above moderating effects highlight the importance of perceived severity, that it indeed has a significant role in influencing computer security behavior, albeit in conjunction with other conditions.

Our findings also indicate that the interaction of perceived severity and perceived susceptibility is not significant. This means that perceived susceptibility has a significant main effect on computer security behavior that is not moderated by perceived severity. It is a direct determinant that operates on its own. The interaction effect of perceived severity and perceived barriers is also not significant. As discussed earlier, this may be because our respondents did not find much inconvenience or barriers in practicing email security.

6.2. Limitations and future work

In this study, one security practice was measured, thus limiting the generalizability of the results to other computer security practices, such as applying system patches or using a strong password. Future studies on other computer security practices could help to uncover the common causal relationships for these computer security practices.

Another limitation is the sample size. Future research could replicate this study using a larger sample size. It would also be useful to compare results obtained from survey respondents who are not as IT-savvy. The determinants of security behavior of such a population may differ.

Cues to action and general security orientation are new concepts that are not previously explored in IS or security behavioral research. Further work is required to explore these concepts. For example, our study measures a subset of possible cues to action. There may be other cues to action, which are significant in motivating a person to adopt security practices. The contingency of these factors is novel and can be further explored with different security practices or with different organizational contexts.

7. Implications and conclusion

7.1. Theoretical implications

For academics, this study reduces the gap in our understanding of user computer security behavior in the context of the organization. Though there are plenty of practical guidelines on improving user behavior suggested by practitioners, their effectiveness has not been investigated. This study helps to address the lack of theoretically-based and empirically validated research in this area. This study assesses the suitability of using a theory from the health domain to explain computer security behavior. Considerable success is achieved giving impetus for future research studies in this area. In particular, the constructs cues to action and general security orientation are new in this area of research. To our best knowledge, no other study has explored the influence of these constructs in security behavior. The constructs perceived susceptibility and perceived severity are also relatively new in IS research. Similar constructs are used in one study [51].

Furthermore, the moderating effects of perceived severity are an important discovery and contribution through the application of the health belief model in the context of computer security. This sheds light on the determinants of computer security behavior and the conditions in which they operate, i.e., that the effects are only significant in the presence of specific conditions. This study has operationalized and extended the popular health belief model to a new area of research. In this way, it has deepened our understanding of human behavior in the face of threats, be it health or security threats. We have also developed and validated items that can be used to measure the constructs of the health belief model applied in the computer security context.

7.2. Practical implications

There are also implications for practitioners in the field of information security awareness program design based on this study. The importance of perceived severity (as a moderator), perceived susceptibility and perceived benefits instructs us on how to design the content for organizational security awareness messages. Indeed, security awareness messages from security-related organizations tend to focus on the susceptibility and severity of consequences and therefore the importance of practicing security. In a content analysis of nine online safety websites (e.g. US-Cert and ISAFE websites), content related to perceived severity and perceived susceptibility are found in all nine websites [27]. When users are aware of the likelihood of threats (perceived susceptibility) and the effectiveness of security controls (perceived benefits), they can make a conscious decision to perform the appropriate preventive behavior. Security awareness programs should focus on educating users about the possibility and damage of security threats and incidents so that users understand the need for security and their roles and responsibilities in protecting organizational data and other information assets. In particular, security awareness messages can be carefully designed to highlight severity and susceptibility. For example, using personalized language such as “You face a 50% chance of being infected by a computer virus” can increase perceived susceptibility [50].

In addition, security awareness programs should train users on the purpose and functions of security controls, be it technical, physical, or human controls. This helps users to understand the benefits of controls and how they mitigate the risk of security threats. The importance of self-efficacy indicates the need for security training so that users are equipped with the confidence in their skills to practice the appropriate security behavior. Security messages should thus be designed to make employees believe that they are able to perform the recommended security behavior [50].

Despite the importance of security awareness and training, our results show that organizational security awareness programs and activities (measured in the construct cues to action) may not be attaining their desired effectiveness. Hence, there is a need to re-look at the design and implementation of security awareness campaigns so that users are effectively educated on threat information and skills to mitigate security threats, thereby improving the security climate of the organization. A customized approach may be needed so that security awareness messages are targeted at individuals with appropriate content and at a suitable level and frequency. Organizations should also consider other means of bringing security messages across to employees, besides using security awareness programs. Deterrence and enforcement measures may complement security awareness activities to improve users' computer security behavior. The interaction effect between cues to action and perceived severity also sheds some light on how to design effective security awareness programs. The severe consequences for security incidents and the implications to self and organization should be emphasized in security awareness messages so that employees understand the severity and the message also acts as a trigger that prompts employees to practice computer security. For example, security messages sent out to employees to patch their systems may be even more effective if the message explains the severity and consequences if the systems are not patched promptly. Emphasizing the severity of security incidents will also motivate employees who are more security-conscious to practice computer security, as suggested by the interaction effect between perceived severity and general security orientation.

Information security of an organization cannot be neglected, and it is clear that technology solutions alone are not sufficient. The security behavior of employees play an important role, and this calls for more research studying the factors that influence individual's decision to practice computer security. This study has uncovered factors that influence safe email behavior through the application of the health belief model. This can help organizations to improve the design of their security awareness program. More can be learnt from the health domain as management attempts to spread the message that everyone has a role to play in information security.

Acknowledgements

This research is supported by the research grant number R-253-000-033-112, School of Computing, National University of Singapore. We thank the editor and the reviewers for their comments and suggestions.

References

[1] C. Abraham, P. Sheeran, The health belief model, in: M. Conner, P. Norman (Eds.), Predicting Health Behaviour, Ch. 2, Open University Press, UK, 2005.

[2] D.V. Ah, S. Ebert, A. Ngamvitroj, N. Park, D.-H. Kang, Predictors of health behaviors in college students, Journal of Advanced Nursing 48 (5) (2004).

[3] I. Ajzen, The theory of planned behavior, Organizational Behavior and Human Decision Processes 50 (1991).

[4] K. Aytes, T. Connolly, A research model for investigating human behavior related to computer security, Proceedings of the Ninth Americas Conference on Information Systems, 2003.

[5] A. Bandura, Self-efficacy: towards a unifying theory of behavioral change, Psychological Review 84 (2) (1977).

[6] V.L. Champion, Instrument development for health belief model constructs, Advances in Nursing Science 6 (3) (1984).

[7] M. Chan, I. Woon, A. Kankanhalli, Perceptions of information security in the workplace: linking information security climate to compliant behavior, Journal of Information Privacy and Security 1 (3) (2005).

[8] W. Chung, H. Chen, W. Chang, S. Chou, Fighting Cybercrime: a review and the Taiwan experience, Decision Support Systems 41 (2006).

[9] G.A. Churchill Jr., A paradigm for developing better measures of marketing constructs, Journal of Marketing Research 6 (1) (1979).

[10] J. Cohen, P. Cohen, S.G. West, L.S. Aiken, Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences, 3rd ed.L/ Erlbaum Associates, Mahwah, N.J., 2003.

[11] D.R. Compeau, C. Higgins, Application of social cognitive theory to training for computer skills, Information Systems Research 6 (2) (1995).

[12] D.R. Compeau, C. Higgins, Computer self-efficacy: development of a measure and initial test, MIS Quarterly 19 (2) (1995).

[13] M. Conner, P. Norman, Predicting health behaviour: a social cognition approach, in: M. Conner, P. Norman (Eds.), Predicting Health Behaviour, Ch. 1, Open University Press, 2005.

[14] F.D. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly 13 (3) (1989).

[15] T. Dinev, Q. Hu, The centrality of awareness in the formation of user behavioral intention toward protective information technologies, Journal of the Association for Information Systems 8 (7) (2007).

[16] J.S. Eccles, A. Wigfield, Motivational beliefs, values, and goals, Annual Review Psychology 53 (2002).

[17] R.F. Falk, N.B. Miller, A Primer for Soft Modeling, The University of Akron Press, Akron, OH, 1992.

[18] L.A. Gordon, M.P. Loeb, W. Lucyshyn, R. Richardson, CSI/FBI Computer Crime and Security Survey, Computer Security Institute, 2006 (July 2006). Accessed 9 Nov 2006 at http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml.

[19] T. Grance, K. Kent, B. Kim, Computer Security Incident Handling Guide, National Institute of Standards and Technology, Jan 2004 Special Publication 800-61. Accessed 29 Sept 2006 at http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf.

[20] G. Groenewold, B. Bruijn, R. Bilsborrow, Migration of the Health Belief Model (HBM): Effects of psychosocial and migrant network characteristics on emigration intentions in five countries in West Africa and the Mediterranean Region, The Population Association of America 2006 Annual Meeting, March 30–April 1, Los Angeles, CA, 2006.

[21] J.F. Hair, R.E. Anderson, R.L. Tatham, W.C. Black, Multivariate Data Analysis, 5th edPrentice-Hall, Englewood Cliffs, NJ, 1998.

[22] A.M. Hedrick, The effects of piracy in foreign markets on U.S. business, Journal of International Business Studies 21 (4) (1990).

[23] J. Jaccard, R. Turrisi, C.K. Wan, Interaction effects in multiple regression, Series: Quantitative Applications in the Social Sciences, No. 72, Sage Publications, Thousand Oaks, CA, 1990.

[24] N.K. Janz, M.H. Becker, The health belief model: a decade later, Health Education Quarterly 11 (1984).

[25] R.K. Jayanti, A.C. Burns, The antecedents of preventive health care behavior: an empirical study, Academy of Marketing Science Journal 26 (1) (1998).

[26] A. Kankanhalli, H.H. Teo, B.C.Y. Tan, K.K. Wei, An integrative study of information systems security effectiveness, International Journal of Information Management 23 (2003).

[27] R. LaRose, N. Rifon, S. Liu, D. Lee, Online safety strategies: a content analysis and theoretical assessment, The 55th Annual Conference of the International Communication Association, New York City, 2005.

[28] R. LaRose, N. Rifon, S. Liu, D. Lee, Understanding online safety behavior: a multivariate model, The 55th Annual Conference of the International Communication Association, New York City, 2005.

[29] R. LaRose, N. Rifon, R. Enbody, Promoting personal responsibility for Internet safety, Communications of the ACM 51 (3) (2008).

[30] S. Milne, P. Sheeran, S. Orbell, Prediction and intervention in health-related behavior: a meta-analytic review of protection motivation theory, Journal of Applied Social Psychology 30 (1) (2000).

[31] G.C. Moore, I. Benbasat, Development of an instrument to measure the perceptions of adopting an information technology innovation, Information Systems Research 2 (1991).

[32] W.L. Neuman, Social Research Methods: Qualitative and Quantitative Approaches, 5th ed.Allyn Bacon, 2003.

[33] B.Y. Ng, M.A. Rahim, A socio-behavioral study of home computer users' intention to practice security, Proceedings of the Ninth Pacific Asia Conference on Information Systems, 7–10 July, Bangkok, Thailand, 2005.

[34] J.C. Nunnally, Psychometric Theory, McGraw-Hill, New York, 1978.

[35] K. Rhodes, Operations security awareness: the mind has no firewall, Computer Security Journal 18 (3) (2001).

[36] R. Richardson, CSI Survey 2007: The 12th Annual Computer Crime and Security Survey, Computer Security Institute, 2007 Accessed 11 October, 2007 at http://www.gocsi.com.

[37] R.N. Rimal, Closing the knowledge–behavior gap in health promotion: the mediating role of self-efficacy, Health Communication 12 (3) (2000).

[38] L. Rogers, Home Computer Security, CERT Coordination Centre, 2002 Accessed 19 September 2006 at http://www.cert.org/homeusers/HomeComputerSecurity/.

[39] I.M. Rosenstock, Why people use health services, The Milbank Memorial Fund Quarterly 44 (3) (1966).

[40] I.M. Rosenstock, The health belief model and preventive health behavior, Health Education Monographs 2 (1974).

[41] I.M. Rosenstock, V.J. Strecher, M.H. Becker, Social learning theory and the health belief model, Health Education Quarterly 15 (1988).

[42] N.C. Schaeffer, S. Presser, The science of asking questions, Annual Review of Sociology 29 (2003).

[43] J.M. Stanton, P.R. Mastrangelo, K.R. Stam, J. Jolton, Behavioral information security: two end user survey studies of motivation and security practices, Proceedings of the Tenth America's Conference on Information Systems, New York, 2004.

[44] G. Stoneburner, A. Goguen, A. Feringa, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, 2002 SP800-30.

[45] D.W. Straub, Validating instruments in MIS research, MIS Quarterly 13 (2) (1989).

[46] D.W. Straub, R.J. Welke, Coping with systems risk: security planning models for management decision making, MIS Quarterly 22 (4) (1998).

[47] M.E. Thomson, R.V. Solms, Information security awareness: educating your users effectively, Information Management and Computer Security 6 (4) (1998).

[48] V.H. Vroom, Work and Motivation, Wiley, New York, 1964.

[49] L.R. Walker, K.W. Thomas, Beyond expectancy theory: an integrative motivational model from health care, Academy of Management Review 7 (2) (1982).

[50] K. Witte, M. Allen, A meta-analysis of fear appeals: implications for effective public health campaigns, Health Education Behavior 27 (5) (2000).

[51] I.M.Y. Woon, G.W. Tan, R.T. Low, A protection motivation theory approach to home wireless security, Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, Nevada, USA, 2005.

[52] W.T. Yue, M. Cakanyilidrim, Y.U. Ryu, D. Liu, Network externalities, layered protection and IT security risk management, Decision Support Systems 44 (2007).

Boon-Yuen Ng is a lecturer and doctoral student in the Department of Information Systems, School of Computing at the National University of Singapore (NUS). She obtained her B.S. (Honors) from the University of California at Berkeley and her M.S. from the University of Illinois at Urbana-Champaign. Her research has been presented in conferences such as the Pacific Asia Conference on Information Systems and the European Conference on Information Systems. Prior to joining NUS, she was an IT consultant with the Infocomm Development Authority of Singapore. She has consulted for several government organizations on information security and policy matters.

Dr. Atreyi Kankanhalli is Assistant Professor in the Department of Information Systems at the National University of Singapore (NUS). She obtained her B. Tech. from the Indian Institute of Technology Delhi, her M.S. from the Rensselaer Polytechnic Institute and Ph. D. from NUS. She had visiting stints at the Haas Business School, University of California Berkeley and the Indian Institute of Science, Bangalore. Prior to joining NUS, she has considerable experience in industrial R & D. She has consulted for several organizations including Bosch SEA and World Bank. Her research interests include knowledge management, IT-enabled organizational forms, and IT in public sector. Dr. Kankanhalli's work has appeared in premium journals such as the MIS Quarterly, Journal of Management Information Systems, IEEE Transactions on Engineering Management, Journal of the American Society for Information Science and Technology, and Decision Support Systems among others. She serves on several editorial boards including IEEE Transactions on Engineering Management and Information and Management. Dr. Kankanhalli was the winner of the ACM-SIGMIS ICIS 2003 Best Doctoral Dissertation award.

Dr. Yunjie (Calvin) Xu is Assistant Professor at the Department of Information System, National University of Singapore. He received his Ph.D. from Syracuse University. His research interest covers knowledge seeking and e-commerce. He has published in the Journal of Association for Information Systems, Communications of the ACM, Journal of the American Society for Information Science and Technology, Electronic Commerce Research and Application, and Information Retrieval.